PR4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593

29177 7590 08/13/2003

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER
KIM, JUNG W

ART UNIT	PAPER NUMBER
2132	13

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

ppg

Office Action Summary	**Application** 09/402,144	**Applicant(s)** HANCK ET AL.
	Examiner Jung W Kim	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____ .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,10-12 and 19-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,10-12 and 19-48* is/are rejected.

7)☒ Claim(s) *3 and 12* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: on page 1, line 10, the sentence is not grammatical; on page 1, line 14, there is an extraneous comma; on page 4 of the amendment "A" prior to action, line 20, the phrase "an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation" should read "an inverse cryptographic operation to form a first commutative checksum from a cryptographic commutative checksum formed by a cryptographic operation"; on page 5, line 24, the word "asymmetric" is misspelled; on page 5, lines 26-28, the disclosure "to ensure cryptographic security" is not a rational for applying an inverse cryptographic method to a cryptographic method; on page 10, line 12, there is an extraneous period. Appropriate correction is required.

2. Claims 3 and 12 are objected to because of the following informalities: in claim 3, the phrase "subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first cryptographic checksum" should read "subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum"; in claim 12, the phrase "an inverse cryptographic operation to form a first cryptographic checksum" should read "an inverse cryptographic operation to form a first commutative checksum". Appropriate correction is required.

Claim Objections

1. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not). Misnumbered claims 21-50 have been renumbered 19-48. As per U.S. practice only the original claim and paper "Amendment 'A' prior to Action" have been entered.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with whi ch it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 28-30 and 43-45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. In said claims, applicant discloses methods and arrangements whereupon digital data is grouped into data segments and furthermore said data segments have no ties to a specific ordering. However, segments without any ties to a specific ordering are essentially independent data and obviate a means for ordering the

segments to reestablish the original digital data. The applicant's disclosure of a grouping of data segments from a digital data and the negation of ordering of said data segments appear to be counteractive actions and requires further elaboration for consideration of enablement.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 1-3, 10-12, 22-27, 31-33, 37-42, and 46-48 are rejected under 35 U.S.C. 102(a) as being anticipated by Halsall, *Data Communications, Computer Networks and Open Systems Fourth Edition* (hereinafter Halsall). As per claim 10, Halsall teaches a block sum check, also known as a two-dimensional parity check, which forms a commutative checksum on digital data. This check covers the arrangement listed in the applicant's claim 10 as explained below:

1) The grouping of the digital data into several data segments by a computer and the formation of a first segment checksum for each data segment is covered by Halsall, page 129, 1st paragraph. The checksum in the example disclosed by Halsall constitutes the assignment of an odd or even parity bit to each block. This step in the process is given the operational name of row parity.

2) The formation of a first commutative checksum by operating on the first segment checksums is covered by Halsall, page 129, 1st paragraph. Halsall teaches a commutative checksum operation by assigning a parity bit (odd or even) for each bit position for all the blocks of a message, including the parity bit position of each block. This step is given the operational name of column parity and the block comprising the column parity bits is the commutative checksum. In addition, Halsall teaches using an XOR operation to establish parity, which is a commutative operation (see Halsall, page 128, Figure 3.14).

3) Furthermore, Halsall teaches cryptographically protecting any message using a cryptographic algorithm (see Halsall, pages 718-719, section 12.4). One encryption method named by Halsall that is typically used on fixed-sized blocks of data is DES (see Halsall, pages 722, section 12.4.3).

4) Finally, Halsall teaches that said arrangement is incorporated into the sending side of a pair of Data Terminal Equipment (DTE) (see Halsall, page 125, section 3.4 and page 128, section 3.4.2). Conventionally, DTE incorporates at least one arithmetic/logic unit; ALUs are the basic units required in hardware to perform arithmetic and logic microoperations.

The aforementioned arrangement covers all of claim 10.

3. A further examination of Halsall will also show to anticipate the arrangement of claim 11. Continuing with the example anticipated by Halsall and outlined in the above claim 10 rejection under 35 U.S.C. 102(a), Halsall covers an arrangement for checking

a predetermined cryptographic commutative checksum. Halsall's arrangement covers the arrangement defined in claim 11 as explained below:

1) The grouping of digital data into a number of data segments by a computer is covered by Halsall, page 129, 1st paragraph.

2) The allocation of the predetermined cryptographic checksum to the digital data and the subjection of said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum are covered by Halsall, page 723, 1st paragraph). Halsall teaches that any message encrypted by DES has an inverse operation (decryption) to retrieve the original message (see Halsall, page 723, 1st paragraph). Furthermore, every ciphertext is associated with a specific plaintext.

3) The formation of a second segment checksum for each data segment, the formation of a second commutative checksum by a commutative operation on the second segment checksums, and a comparison of the first commutative checksum and the second commutative checksum for a match are covered by Halsall, page 129, Figure 3.15 (b).

4) Furthermore, Halsall teaches that said arrangement is incorporated into the receiving side of a pair of DTEs and conventionally, DTEs incorporate at least one arithmetic/logic unit (see Halsall, page 125, section 3.4 and page 128, section 3.4.2). The aforementioned arrangement anticipates all of claim 11.

4. The above arrangements covered in the claims 10 and 11 rejections under 35 U.S.C. 102(a) combine to cover the arrangement outlined in claim 12.

5. As per claims 37-39, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined in the above claims 10, 11, and 12 rejections under 35 U.S.C. 102(a). In addition, as mentioned previously, the cryptographic operations described use a symmetric key methodology (see Halsall, page 723, 1st paragraph).

6. As per claims 40-42, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined in the above claims 10, 11, and 12 rejections under 35 U.S.C. 102(a). In addition, Halsall teaches that the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (see Halsall, page 127, section 3.4.1); the XOR operation exhibits both commutative and associative properties. Furthermore, it is known in the art that controlling the data inputs to the arithmetic circuits of the ALU determines the type of operation executed by the ALU. In the arrangements covered by Halsall, the circuits would be arranged to implement the XOR operation.

7. As per claims 46-48, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined in the above claim 10, 11, and 12 rejections under 35 U.S.C. 102(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since the ISO architecture is the standard reference model for any digital network, the digital data would be processed in accordance with the protocols defined in the network layer.

8. As per claims 1-3, 22-27, and 31-33 (hereinafter claims A), they are method claims corresponding to claims 10-12, 37-42, and 46-48 (hereinafter claims B) and they do not teach or define above the information claimed in claims B and is therefore rejected under Halsall for claims A for the same reasons set forth in the rejections of claims B.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 19-21 and 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halsall. As per claims 34-36, Halsall covers the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined in the above claim 10, 11, and 12 rejections under 35 U.S.C. 102(a). However, the parity check described in the aforementioned methods for forming the segment checksums are not in accordance with a type from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function as specified in the applicant's claims. In a separate section, Halsall does teach that a CRC code is used in lieu of the parity check for more reliable detection of transmission errors such as burst errors (see Halsall, page 130, section 3.4.3). It would be obvious to one of ordinary skill in the art at the time the invention was made to form the segment checksums using CRC instead of parity checking. The motivation for using CRC in the 3 arrangements would be to provide more reliable detection of transmission errors for each segment as taught in the separate section of Halsall.

3. As per claims 19-21, they are method claims corresponding to claims 34-36 and they do not teach or define above the information claimed in claims 19-21 and is therefore rejected under Halsall for claims 19-21 for the same reasons set forth in the rejections of claims 34-36.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Fischer E.U. Patent Application No. 94303430.6 discloses a method for updating the hash value of a data file.

Bellare U.S. Patent No. 5,673,318 discloses a method and apparatus for data authentication in a data communication environment.

Kemmetmeuller U.S. Patent No. 4,183,463 discloses a method for RAM error correction using two dimensional parity checking.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is 703-305-8289. The examiner can normally be reached on M-F 8:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-9939 for regular communications and 703-746-9939 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Jung W Kim
Examiner
Art Unit 2132

jk
August 6, 2003

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100